Europ. J. Combinatorics (1999) **20**, 647–662
Article No. eujc.1999.0313
Available online at http://www.idealibrary.com on IDEAL

Completely Transitive Codes in Hamming Graphs

MICHAEL GIUDICI† AND CHERYL E. PRAEGER

A *code* in a graph Γ is a non-empty subset C of the vertex set V of Γ. Given C, the partition of V according to the distance of the vertices away from C is called the *distance partition of* C. A *completely regular code* is a code whose distance partition has a certain regularity property. A special class of completely regular codes are the *completely transitive codes*. These are completely regular codes such that the cells of the distance partition are orbits of some group of automorphisms of the graph. This paper looks at these codes in the Hamming Graphs and provides a structure theorem which shows that completely transitive codes are made up of either *transitive* or *nearly complete*, completely transitive codes. The results of this paper suggest that particular attention should be paid to those completely transitive codes of transitive type.

1. INTRODUCTION

A *code* C in the graph Γ is a non-empty subset of the vertex set V of Γ. In keeping with the motivation of error-correcting codes, we refer to vertices in the code as *codewords*. The *trivial code* is the code consisting of a single codeword while the *complete code* is the code consisting of all the vertices of Γ. We note that an error-correcting code of length m over a field of size q can be considered as a code in the corresponding Hamming Graph $H(m, q)$ (which will be defined below). We define the *covering radius* of C as

$$t = \max\{d(\alpha, C) : \alpha \in V\},$$

where $d(\alpha, C)$ is the *distance between* α *and the code* C given by $d(\alpha, C) = \min\{d(\alpha, \beta) : \beta \in C\}$. For $0 \leq i \leq t$, we define

$$C_i = \{\alpha \in V : d(\alpha, C) = i\}.$$

The set $\{C_0 = C, C_1, \ldots, C_t\}$ partitions V and is known as the *distance partition of* C, and the C_i are called its *cells*. We also define the minimum distance of a code C to be

$$\delta = \min\{d(\alpha, \beta) : \alpha, \beta \in C, \alpha \neq \beta\}.$$

A partition $\{B_1, \ldots, B_r\}$ of V is *equitable* if, for all i and j, the number of neighbours of a vertex in B_i, in the cell B_j, is independent of the vertex chosen in B_i. We then say that a code C is *completely regular* if the distance partition of C is equitable. This definition is the one used by Godsil [6, p. 208] and was proved by Neumaier in [9] to be equivalent to that given in [2, p. 346]. These codes are of great interest because in distance regular graphs, all perfect codes are completely regular, (see [9]).

A special class of completely regular codes is the class of completely transitive codes. We say that a code in the graph Γ is *completely transitive* if there exists a subgroup G of the group of automorphisms of Γ, such that each cell C_i in the distance partition of C is an orbit of G. If we wish to specify the group G, we say that C is *G-completely transitive*. This definition was introduced by Godsil and the second author in [7], where they studied completely transitive

†Current address: School of Mathematical Sciences, Queen Mary and Westfield College, Mile End Road, London E1 4NS, U.K.

0195–6698/99/070647 + 16 $30.00/0

codes in the Johnson Graphs. Clearly, a completely transitive code is completely regular. Patrick Solé [10] gave a different definition for completely transitive codes in the case of linear binary codes. We will extend this definition to the case of any linear code and from now on will call such a code *coset-completely transitive*. We discuss this definition in Section 3, where for any linear code we define the group $N_C.\mathrm{Aut}(C)$ associated with C and prove the following theorem:

THEOREM 1.1. *Let C be a linear code in the graph $H(m, q)$. Then C is coset-completely transitive if and only if C is $N_C.\mathrm{Aut}(C)$-completely transitive.*

Then in the case of binary and ternary linear codes we can extend this result to:

THEOREM 1.2. *Let C be a binary or ternary linear code. Then C is completely transitive if and only if C is coset-completely transitive.*

We show in Example 3.1 that the assertion of Theorem 1.2 is false for prime powers $q \geq 7, q \neq 8$.

In this paper we look at completely transitive codes in the Hamming Graphs. The vertices of the Hamming Graph $H(m, q)$ are the m-tuples with entries from a set Q of size q. Two vertices are joined by an edge if and only if they differ in exactly one entry. The automorphism group $\mathrm{Aut}(\Gamma)$ of the Hamming Graph $\Gamma = H(m, q)$ is the wreath product $S_q \mathrm{wr} S_m$ ([2, Theorem 9.2.1]); $\mathrm{Aut}(\Gamma)$ is a semidirect product $N.H$ where for $g = (g_1, \ldots, g_m) \in N \cong S_q^m$, and $\sigma \in H \cong S_m$ we have:

$$\alpha^g = (\alpha_1^{g_1}, \ldots, \alpha_m^{g_m}),$$
$$\alpha^\sigma = (\alpha_{1\sigma^{-1}}, \ldots, \alpha_{m\sigma^{-1}}),$$

for all vertices $\alpha = (\alpha_1, \ldots, \alpha_m) \in V$. The map $g\sigma \mapsto \sigma$ defines a natural homomorphism $\tau : \mathrm{Aut}(\Gamma) \to H$ and the image $H \cong S_m$ is the group of permutations of the entries of the m-tuples.

In Section 4 we define two types of codes; *G-transitive* and *G-nearly-complete* (Definition 4.1) codes. Then in Section 5 we prove the following theorem which shows that completely transitive codes are essentially one of these two types:

THEOREM 1.3. *An incomplete code C in the Hamming graph $H(m, q)$ is completely transitive if and only if there exists i such that $1 \leq i \leq m$ and, rearranging the entries if necessary, $C = \overline{C} \times Q^{m-i}$ where $\overline{C}$ is a completely transitive code in $H(i, q)$ which is transitive or nearly complete.*

In Section 6, we investigate the structure of G-nearly-complete, G-completely transitive codes. To do this, we introduce the concept of a *section $C(\beta, J)$ of a code C relative to a codeword β and a subset of entries J* (Definition 6.1). This process is similar to the formation of a contraction of a design (see [1, p. 67]). It turns out that for any completely transitive code C, we can find a section which is a completely transitive code of transitive type.

THEOREM 1.4. *Let C be a completely transitive code in the graph $H(m, q)$. Then there exists a section $C(\beta, J)$ relative to a subset J of entries and a codeword β such that $C(\beta, J)$ is a completely transitive code of transitive type in $H(|J|, q)$.*

This last result suggests that particular attention needs to be paid to the examples of transitive type. We begin this task in a sequel to this paper. The results in Section 5 were part of the honours dissertation of the first author while the results of Sections 3 and 6 form a part of the the first author's master's thesis [5].

2. PRELIMINARIES

First, we verify that completely transitive codes are completely regular.

LEMMA 2.1. *If a code C in a graph Γ is G-completely transitive, for some $G \leqslant \mathrm{Aut}(\Gamma)$, C is completely regular.*

PROOF. Let t be the covering radius of C and then let $0 \leq i \leq t$. Then as C_i is a G-orbit, for all $\alpha, \beta \in C_i$ there exists a $g \in G$ such that $\alpha^g = \beta$. Hence, for all j, $C_j \cap \Gamma(\alpha)$ and $C_j \cap \Gamma(\beta) = (C_j \cap \Gamma(\alpha))^g$ have the same cardinality. This means that the distance partition of C is an equitable partition, so C is a completely regular code. □

The next lemma follows immediately from the definition of a completely transitive code, and its proof is omitted. For a group G acting on a set V, and a subset C of V, G_C denotes the setwise stabilizer of C in G.

LEMMA 2.2. *A code C in a graph Γ is G-completely transitive for some $G \leqslant \mathrm{Aut}(\Gamma)$ if and only if C is an $(\mathrm{Aut}(\Gamma)_C)$-completely transitive code.*

We also have the following lemma essentially from [7]:

LEMMA 2.3. *Let C be a code in the graph Γ with covering radius t. Then C is G-completely transitive if and only if C_t is G-completely transitive.*

So completely transitive codes arise in pairs. It will sometimes be convenient to extend the notation for completely transitive codes as follows:

DEFINITION. Let C be a code in the graph Γ and let G be a group. We say that C is *G-completely transitive* if there exists a permutation representation

$$\varphi : G \longrightarrow \mathrm{Aut}(\Gamma),$$

such that C is $(G)\varphi$-completely transitive.

If confusion over the permutation representation may occur, we will state which one we are using.

3. COSET-COMPLETELY TRANSITIVE CODES

Let C be a linear code of length m over a field of size q. If $q = 2$, the *automorphism group* $\mathrm{Aut}(C)$ *of* C as a linear code is the stabilizer in S_m of the code C. If q is prime, then we define $\mathrm{Aut}(C)$ to consist of all monomial matrices in $GL(m, q)$ which fix C setwise, that is, the largest subgroup of $\mathbb{F}_q^* \mathrm{wr} S_m$ which stabilizes C. Here $\mathbb{F}_q^*$ acts on $Q = \mathbb{F}_q$ by multiplication. Note that the binary case is just a special case of this as $\mathbb{F}_2^* = 1$ and so the monomial matrices in $GL(m, 2)$ are just the permutation matrices of degree m. If q is a proper power of a prime, then we allow $\mathrm{Aut}(C)$ to also include any field automorphisms of the coresponding field $\mathbb{F}_q$ which fix our code C. That is, $\mathrm{Aut}(C)$ is the largest subgroup of $(\mathbb{F}_q^* \mathrm{wr} S_m).\mathrm{Aut}\mathbb{F}_q$ which fixes C setwise. (See [8, Chap. 8, Section 5].)

Now as C is linear, it is disjoint from each of its additive cosets $\boldsymbol{x} + C$ distinct from C ($\boldsymbol{x} \in \mathbb{F}_q^m$). Moreover, $\mathrm{Aut}(C)$ induces an action on the set of cosets of C in the following way; for all $\sigma \in \mathrm{Aut}(C)$ and for every vertex $\boldsymbol{x} \in \mathbb{F}_q^m$,

$$(\boldsymbol{x} + C)^\sigma = \boldsymbol{x}^\sigma + C.$$

Solé's concept of a completely transitive binary linear code, introduced in [10] was:

DEFINITION. Let C be a binary linear code with covering radius t. Then C is *coset-completely transitive* if $\mathrm{Aut}(C)$ has $t+1$ orbits on the cosets of C.

We now extend this definition to a linear code over any finite field.

DEFINITION. Let C be a linear code with covering radius t. Then C is *coset-completely transitive* if $\mathrm{Aut}(C)$ has $t+1$ orbits on the cosets of C.

If C is coset-completely transitive, then C is not usually $\mathrm{Aut}(C)$-completely transitive by our definition. This is because $\mathrm{Aut}(C)$ is often not even transitive on C, for example, when C has codewords of different weights. To show that Solé's definition is equivalent to ours, we need to find some larger group G corresponding to C such that C is G-completely transitive.

For $\boldsymbol{v} = (v_1, \ldots, v_m) \in \mathbb{F}_q^m$, define $g_{\boldsymbol{v}} = (g_1, \ldots, g_m) \in S_q^m$ to be the translation by $\boldsymbol{v}$, that is, for all $\boldsymbol{u} \in \mathbb{F}_q^m$ the image of $\boldsymbol{u}$ under $\boldsymbol{v}$ is $\boldsymbol{u} + \boldsymbol{v}$. In fact, in the case where $q = 2$, each $g \in S_2^m$ is equal to $g_{\boldsymbol{v}}$ for some $\boldsymbol{v} \in \mathbb{F}_2^m$. For a linear code C, we define

$$N_C = \{g_{\boldsymbol{c}} : \boldsymbol{c} \in C\},$$

the set of all translations of $\mathbb{F}_q^m$ by vectors in C. Note that N_C is a subgroup since C is linear. We now have the following lemma.

LEMMA 3.1. *If C is a linear code in $\mathbb{F}_q^m$ then:*

(1) $N_C \leqslant S_q^m$.
(2) $\mathrm{Aut}(C)$ *normalizes* N_C.
(3) $G = N_C.\mathrm{Aut}(C) \leqslant S_q^m.S_m$.
(4) G *fixes* C *setwise.*
(5) *The* N_C*-orbits are the cosets of* C*; in particular,* C *is a* G*-orbit.*
(6) *If* $q = 2$ *or* 3, G *is the stabilizer in* $S_q \mathrm{wr} S_m$ *of* C.

PROOF. (1) As C is a subspace of $\mathbb{F}_q^m$, $\mathbf{0} \in C$ and so $1 \in N_C$. Also, for all $g_c, g_b \in N_C$, we have that $g_{\boldsymbol{c}} g_{\boldsymbol{b}} = g_{\boldsymbol{c}+\boldsymbol{b}}$. As C is a subspace, $\boldsymbol{c} + \boldsymbol{b} \in C$ and so $g_{\boldsymbol{c}+\boldsymbol{b}} \in N_C$. For all $g_{\boldsymbol{c}} \in N_C$, as C is a subspace, $g_{-\boldsymbol{c}} \in N_C$ and $g_{\boldsymbol{c}} g_{-\boldsymbol{c}} = g_{\boldsymbol{c}-\boldsymbol{c}} = 1$. Hence N_C is a subgroup of S_q^m.

(2) Let $\sigma \in \mathrm{Aut}(C)$, $g_{\boldsymbol{c}} \in N_C$, and set $\boldsymbol{b} = \boldsymbol{c}^\sigma$. Then $\boldsymbol{b} \in C$ since $\sigma \in \mathrm{Aut}(C)$. Also, since σ preserves addition, a straightforward computation shows that $\sigma^{-1} g_{\boldsymbol{c}} \sigma$ maps each m-tuple $\boldsymbol{u}$ to $\boldsymbol{u} + \boldsymbol{b}$, that is, $\sigma^{-1} g_{\boldsymbol{c}} \sigma = g_{\boldsymbol{b}}$. Hence $\mathrm{Aut}(C)$ normalizes N_C.

(3) Since $\mathrm{Aut}(C)$ normalizes N_C, the set $G = N_C.\mathrm{Aut}(C)$ forms a semidirect product and so $G \leqslant S_q^m.S_m$.

(4) As each element of N_C acts on C by translating by a codeword in C and since C is a subspace, N_C fixes C setwise. Then, since $\mathrm{Aut}(C)$ also fixes C setwise by definition, $G = N_C.\mathrm{Aut}(C)$ fixes C setwise.

(5) Clearly N_C fixes each coset of C setwise. Let $\boldsymbol{x}, \boldsymbol{y} \in \boldsymbol{v} + C$. Then $\boldsymbol{y} - \boldsymbol{x} \in C$ and so $g_{\boldsymbol{y}-\boldsymbol{x}} \in N_C$. Also $\boldsymbol{x}^{g_{\boldsymbol{y}-\boldsymbol{x}}} = \boldsymbol{x} + \boldsymbol{y} - \boldsymbol{x} = \boldsymbol{y}$. Hence N_C is transitive on $\boldsymbol{v} + C$ and so C is an N_C-orbit. Also since G fixes C setwise, C is a G-orbit.

(6) Let H be the stabilizer in $S_q \mathrm{wr} S_m$ of C. Then as G fixes C setwise, $G \leqslant H$. Suppose that $H \neq G$. Then there exists $g\sigma \in H \backslash G$ where $g \in S_q^m$ and $\sigma \in S_m$. Now $g\sigma : \mathbf{0} \mapsto \boldsymbol{x}$ for some $\boldsymbol{x} \in C$, and $g_{-\boldsymbol{x}} \in N_C$ maps $\boldsymbol{x}$ to $\mathbf{0}$. Hence the permutation $g\sigma g_{-\boldsymbol{x}}$ fixes $\mathbf{0}$, and $g\sigma g_{-\boldsymbol{x}} \in H \backslash G$. Thus, there exists $g'\sigma' \in H \backslash G$ which fixes $\mathbf{0}$. If $q = 2$, then $g' \in S_2^m$ and so $g' = g_{\boldsymbol{v}}$ for some $\boldsymbol{v} \in \mathbb{F}_2^m$. Thus

$$g'\sigma' : \mathbf{0} \mapsto (\mathbf{0} + \boldsymbol{v})^{\sigma'} = \mathbf{0},$$

and hence $\boldsymbol{v} = \mathbf{0}$, so $\sigma' \in H \cap S_m = \mathrm{Aut}(C)$. Therefore $g'\sigma' \in G$; a contradiction. Hence $H = G$. If $q = 3$, then

$$g'\sigma' : \mathbf{0} \mapsto (\mathbf{0}^{g'})^{\sigma'} = \mathbf{0},$$

and hence g' fixes $\mathbf{0}$. So $g' \in (\mathbb{F}_3^*)^m$ and hence $g'\sigma' \in (\mathbb{F}_3^* \mathrm{wr} S_m) \cap H = \mathrm{Aut}(C)$. Therefore $g'\sigma' \in G$; a contradiction. Hence $H = G$. □

We now use this lemma to prove the following theorem which shows that coset-completely transitive, linear codes are completely transitive under our definition. We also prove a partial converse: if C is G-completely transitive with $G \leqslant N_C.\mathrm{Aut}(C)$ (that is, for G involving only translations and 'linear' automorphisms), then C is coset-completely transitive. The forward implication in the binary case was proved in [4, Theorem 4.5.3]. Theorem 1.1 follows immediately from it.

THEOREM 3.1. *Let C be a linear code in the graph $\Gamma = H(m, q)$ where q is a prime power. Then C is coset-completely transitive if and only if C is $(N_C.\mathrm{Aut}(C))$-completely transitive.*

PROOF. Let $\{C, C_1, \ldots, C_t\}$ be the distance partition of the vertices of $H(m, q)$ determined by C. Let $\boldsymbol{x} \in C_i$. Then $\boldsymbol{x}$ differs from some codeword $\boldsymbol{b}$ say, in i coordinates and this is the smallest such distance between $\boldsymbol{x}$ and any codeword. Thus, for all $\boldsymbol{c} \in C$ we have that $d(\boldsymbol{x}+\boldsymbol{c}, \boldsymbol{b}+\boldsymbol{c}) = i$ and hence since $\boldsymbol{b}+\boldsymbol{c} \in C$ as C is linear, we have that $d(\boldsymbol{x}+\boldsymbol{c}, C) \leq i$. Now suppose that $d(\boldsymbol{x}+\boldsymbol{c}, C) = j < i$. Then there exists $\boldsymbol{d} \in C$ such that $d(\boldsymbol{x}+\boldsymbol{c}, \boldsymbol{d}) = j$. However this implies that $d(\boldsymbol{x}, \boldsymbol{d}-\boldsymbol{c}) = j$ and $\boldsymbol{d}-\boldsymbol{c} \in C$ as C is linear. Therefore $d(\boldsymbol{x}, C) \leq j < i$ which is a contradiction and so $d(\boldsymbol{x}+\boldsymbol{c}, C) = i$ for all $\boldsymbol{c} \in C$, that is, the coset $\boldsymbol{x}+C$ is contained in the cell C_i. Thus each C_i is a union of complete cosets of C, and each C_i is fixed setwise by $N_C.\mathrm{Aut}(C)$.

Suppose that C is coset-completely transitive, so the number of orbits of $\mathrm{Aut}(C)$ on cosets is $t+1$. Hence the set of cosets of C in C_i forms an orbit of $\mathrm{Aut}(C)$ on C-cosets. Also from Lemma 3.1, each coset of C is an N_C-orbit, and hence $N_C.\mathrm{Aut}(C)$ is transitive on each C_i. So C is $(N_C.\mathrm{Aut}(C))$-completely transitive.

Conversely, suppose that C is $(N_C.\mathrm{Aut}(C))$-completely transitive. Then $N_C.\mathrm{Aut}(C)$ has $t+1$ orbits on $\mathbb{F}_q^m$ and hence $\mathrm{Aut}(C)$ has $t+1$ orbits on the cosets of C. So C is coset-completely transitive. □

We can now prove the following theorem which shows that in the case where $q = 2$ or 3 and C is linear, the two definitions of completely transitive codes are equivalent. Theorem 1.2 follows immediately.

THEOREM 3.2. *Let C be a linear code in the graph $H(m, q)$ where $q = 2$ or 3. Then C is coset-completely transitive if and only if C is completely transitive.*

PROOF. The forward implication was proved in Theorem 3.1. If there exists $G \leqslant S_q \mathrm{wr} S_m$ such that C is G-completely transitive, by Lemma 2.2, C is H-completely transitive, where H is the stabilizer in $S_q \mathrm{wr} S_m$ of C. Also, by Lemma 3.1, $H = N_C.\mathrm{Aut}(C)$ and so, by Theorem 3.1, C is coset-completely transitive. □

Theorem 3.2 does not hold for all q, as when $q \geq 4$ we cannot guarantee that the stabilizer of C in $S_q \mathrm{wr} S_m$ is $N_C.\mathrm{Aut}(C)$. We have the following family of examples of completely transitive linear codes which are not coset-completely transitive.

EXAMPLE 3.1. Let $q \geq 7$ be a power of a prime p, with $q \neq 8$ and let C be the repetition code in $\mathbb{F}_q^3$, that is, $C = \{(a, a, a) : a \in \mathbb{F}_q\}$. Then

$$C_1 = \{(b, a, a), (a, b, a), (a, a, b) : a, b \in \mathbb{F}_q^m \text{ and } a \neq b\},$$

and

$$C_2 = \{(a, b, c) : a \neq b \neq c \neq a\}.$$

Let $G = S_q.S_3$ where $g \in S_q$ maps $(x_1, x_2, x_3) \in \mathbb{F}_q^3$ to (x_1^g, x_2^g, x_3^g). Then, as S_q acts 3-transitively on $\mathbb{F}_q$, the orbits of G are C, C_1 and C_2. Hence C is G-completely transitive.

Now $\mathrm{Aut}(C) = \mathbb{F}_q^*.S_3\mathrm{Aut}\mathbb{F}_q$ where $\mathbb{F}_q^*$ acts on $\mathbb{F}_q^3$ by scalar multiplication, that is, $\lambda \in \mathbb{F}_q^*$ maps $\boldsymbol{x} \in \mathbb{F}_q^3$ to $\lambda\boldsymbol{x}$. The cosets of C contained in C_1 are all of those cosets of the form $(a, 0, 0) + C$, $(0, a, 0) + C$ and $(0, 0, a) + C$ where $a \in \mathbb{F}_q^*$. There are $3(q - 1)$ such cosets and so there are $q^2 - 3(q - 1) - 1 = (q - 2)(q - 1)$ cosets of C contained in C_2. Now $|\mathrm{Aut}(C)| = 6(q - 1)\log_p q$ and so if $\mathrm{Aut}(C)$ had the set of cosets of C contained in C_2 as an orbit on cosets, we would have that $(q - 2)(q - 1)$ divides $6(q - 1)\log_p q$. However, this does not happen for $q \geq 7$, $q \neq 8$ and so C is not coset-completely transitive.

4. EXAMPLES OF COMPLETELY TRANSITIVE CODES

Before providing some examples of completely transitive codes in the Hamming Graphs, we introduce some notation for the vertex set. We denote the vertex set of the graph $H(m, q)$ by $Q_1 \times \cdots \times Q_m = Q^m$ where $Q = \{1, \ldots, q\}$. We also denote the set of entries $\{1, \ldots, m\}$ by M. For $J \subseteq M$, we write

$$Q^J = \prod_{j \in J} Q_j. \tag{1}$$

Then we define the graph $H(J, q)$ as the Hamming Graph with vertex set Q^J (and two vertices are adjacent if and only if they differ in one coordinate). Note that $H(J, q)$ is isomorphic to $H(|J|, q)$.

As the Hamming Graphs are distance transitive, the trivial code, $C = \{\alpha\}$ is G-completely transitive with G the stabilizer in $S_q\mathrm{wr}S_m$ of the vertex α.

EXAMPLE 4.1. By Theorem 3.1, the examples provided by Solé in [10] provide us with examples of completely transitive codes. So we have the following examples of G-completely transitive codes in the Hamming Graphs:

(1) The binary Hamming code C of length $2^r - 1$ with $G = N_C.GL(r, 2)$;
(2) The extended binary Hamming code C of length 2^r with $G = N_C.AGL(r, 2)$;
(3) The binary Golay code C with $G = N_C.M_{23}$;
(4) The extended binary Golay code C with $G = N_C.M_{24}$;

where the group N_C is the group of translations by codewords in C.

Using our extension of the definition of coset-completely transitive codes we can also show that the following are completely transitive.

(1) The Hamming code C of length $(q^r - 1)/(q - 1)$ over a field of size q. Here C is a perfect, single error-correcting code and so $t = 1$ and the coset representatives for the cosets of C can be chosen to be all of weight one. C is a cyclic code so $\mathrm{Aut}(C)$ is transitive on entries and as C is a linear code, it is fixed by scalar multiplication. Thus $\mathrm{Aut}(C)$ is transitive on cosets distinct from C.

(2) The ternary Golay code C of length 12. From [8, p. 645] we obtain the generators of the automorphism group of C and then via a MAGMA ([3]) calculation we can determine that $\mathrm{Aut}(C)$ is transitive on cosets.
(3) The perfect ternary Golay code C of length 11. The automorphism group of this code is the stabilizer of one coordinate in the automorphism group of the extended ternary Golay code. This can then be determined from above and then another MAGMA ([3]) calculation gives us the fact that $Aut(C)$ is transitive on cosets.

We now define two types of codes. For $I \subseteq M$ let

$$\Pi_I : Q^m \to Q^I$$

denote the natural projection.

DEFINITION. Let G be a group and let C be a G-invariant code in the graph $H(m, q)$ under the permutation representation:

$$\varphi : G \longrightarrow \mathrm{Aut}(H(m, q)).$$

We say that C is *G-transitive* if the action of $\varphi(G)$ on entries is transitive. We say that C is *G-nearly-complete* if C is not of transitive type and, for every proper G-invariant subset I of M, we have $\Pi_I(C) = Q^I$.

The examples provided in Example 4.1 are examples of G-transitive, G-completely transitive codes.

We now provide several examples of G-nearly-complete, G-completely transitive codes.

EXAMPLE 4.2. Let C be the repetition code $\{(\delta, \delta) : \delta \in Q^n\}$ in the graph $H(2n, q)$ and let $G = \{(g, g) : g \in S_q \mathrm{wr} S_n\}$.

Now G fixes C setwise and has orbits $\{1, \ldots, n\}$ and $\{n+1, \ldots, 2n\}$ on entries; hence C is G-nearly-complete. Also, C is an orbit of G in $H(2n, q)$ as $S_q \mathrm{wr} S_n$ is transitive on Q^n. Then, for all $i = 0, \ldots, t$, each C_i is G-invariant.

Let $i = 1, \ldots, t$, and let $(\delta, \gamma) \in C_i$. Then there exists $(\lambda, \lambda) \in C$ such that $d((\delta, \gamma), (\lambda, \lambda)) = i$. Therefore, $d(\lambda, \delta) = k$ and $d(\gamma, \lambda) = l$ where $k + l = i$ and so $d(\delta, \gamma) \leq k + l = i$. However if $d(\delta, \gamma) = j < i$, we have that $d((\delta, \gamma), (\delta, \delta)) = j$ and so $d(C, (\delta, \gamma)) \leq j < i$ which is a contradiction. Therefore $d(\delta, \gamma) = i$ and so $C_i \subseteq \{(\delta, \gamma) : d(\delta, \gamma) = i\}$ for all i. Now suppose that $d(\delta, \gamma) = d(\xi, \eta) = i$. Then as $H(n, q)$ is a distance transitive graph, there exists $g \in S_q \mathrm{wr} S_n$ such that $(\delta^g, \gamma^g) = (\xi, \eta) = (\delta, \gamma)^{\overline{g}}$ where $\overline{g} = (g, g) \in G$. Therefore $C_i = \{(\delta, \gamma) : d(\gamma, \delta) = i\}$ and each C_i is a G-orbit. Hence C is a G-nearly-complete, G-completely transitive code of covering radius $t = n$. By Lemma 2.3, C_t is also a G-completely transitive code, and C_t is also G-nearly-complete.

EXAMPLE 4.3. Let $C = \{(\alpha_1, \ldots, \alpha_m) : \sum_{i=1}^m \alpha_i = 0\}$ be a code in the graph $H(m, q)$ where q is a power of a prime and we take Q to be the field $\mathbb{F}_q$. Then for all $j = 1, \ldots, m$, we have that $\Pi_{M \setminus j}(C) = Q^{M \setminus j}$. Thus C will be G-nearly-complete for any G which fixes C setwise and is intransitive on M.

Let $\alpha \in C$ and let β be any vertex in $H(m, q)$. Then

$$\alpha + \beta = (\alpha_1 + \beta_1, \ldots, \alpha_m + \beta_m),$$

and if $\beta \in C$ then $\alpha + \beta \in C$ as $\sum(\alpha_i + \beta_i) = \sum \alpha_i + \sum \beta_i = 0$. For all $\alpha \in Q^m$, let $g_\alpha \in S_q^m$ denote 'translation by α', that is $g_\alpha : \beta \mapsto \beta + \alpha$. Then

$$N = \{g_\alpha : \alpha \in Q^m\} \leqslant S_q^m,$$

and also

$$N_C = \{g_\alpha : \alpha \in C\} \leqslant S_q^m.$$

Now for all α and $\beta \in C$, let $\gamma = \beta - \alpha$. Then $\gamma \in C$ as $\sum(\beta_i - \alpha_i) = \sum \beta_i - \sum \alpha_i = 0$. So $\alpha^{g_\gamma} = \alpha + \beta - \alpha = \beta$. Therefore N_C is transitive on C.

As $\Pi_{M\setminus j}(C) = Q^{M\setminus j}$, we have that $t = 1$. Therefore for all α such that $\sum \alpha_i \neq 0$, α must belong to C_1.

Now the subgroup $H = N.(\mathbb{F}_q^* \mathrm{wr} S_m)$ of $S_q \mathrm{wr} S_m$ preserves the structure of $H(m, q)$ as an m-dimensional vector space over $\mathbb{F}_q$, and the subgroup of H which leaves C invariant is $N_C.\mathbb{F}_q^*.S_m$ where $\lambda \in \mathbb{F}_q^*$ acts as scalar multiplication, $\lambda : \beta \mapsto \lambda\beta$.

Now let $\alpha, \beta \in C_1$. Then $\sum \alpha_i = k$ and $\sum \beta_i = l$ for some $k, l \in \mathbb{F}_q^*$. Now there exists $\mu \in \mathbb{F}_q^*$ such that $k\mu = l$ and hence $\sum(\beta_i - \mu\alpha_i) = 0$, so $\gamma := \beta - \mu\alpha \in C$. Then $(\mu\alpha)^{g_\gamma} = \beta$ and so $H_C = N_C.\mathbb{F}_q^*$ is transitive on C_1. So C is an H_C-completely transitive code in $H(m, q)$. Also for all $\sigma \in S_m$ we have that $C^\sigma = C$. Now choose any $L \leqslant S_m$ with orbits $I_1, \ldots, I_s$ on M and let $G = H_C.L$. Then if $s = 1$, C is a G-transitive, G-completely transitive code, while if $s \geq 2$, C is a G-nearly-complete, G-completely transitive code. Also, by Lemma 2.3, C_1 is a G-completely transitive code which is either G-transitive or G-nearly-complete depending on s.

5. Projecting Codes

For a code C and a subset $I = \{i_1, \ldots, i_k\} \subseteq M$, $\Pi_I(C)$ is a code in the graph $H(I, q)$. If C has covering radius t, then $\Pi_I(C)$ has distance partition $\{\Pi_I(C), (\Pi_I(C))_1, \ldots, (\Pi_I(C))_r\}$ for some $r \leq t$. First we relate the distance partitions of C and $\Pi_I(C)$.

Lemma 5.1. *Let C be a code in $H(m, q)$, then for all $i = 0, \ldots, t$, $(\Pi_I(C))_i \subseteq \Pi_I(C_i)$.*

Proof. Without loss of generality, we can take I to be $\{1, \ldots, k\}$. Then for all $\alpha = (\alpha_1, \ldots, \alpha_k) \in (\Pi_I(C))_i$, there exists $\beta = (\beta_1, \ldots, \beta_k) \in \Pi_I(C)$ such that $d(\alpha, \beta) = i$ and i is the smallest distance between α and any point in $\Pi_I(C)$. So there exists $\beta' = (\beta_1, \ldots, \beta_k, \beta'_{k+1}, \ldots, \beta'_m) \in C$. Let $\alpha' = (\alpha_1, \ldots, \alpha_k, \beta'_{k+1}, \ldots, \beta'_m)$. Then $d(\alpha', \beta') = i$ and $\Pi_I(\alpha') = \alpha$. Moreover, $d(\alpha', C) = i$ since, if $\alpha' \in C_j$, for some $j < i$, then $d(\alpha, \Pi_I(C)) \leq j$ which contradicts $\alpha \in (\Pi_I(C))_i$. Therefore $\alpha' \in C_i$. Thus $(\Pi_I(C))_i \subseteq \Pi_I(C_i)$. □

If C is a G-completely transitive code, we want to be able to carry the group information with us when we project our code. We do this by choosing I to be G-invariant. Then we can define a permutation representation ρ_I of G on $H(I, q)$ by:

$$\begin{aligned} \rho_I(g) : H(I, q) &\longrightarrow H(I, q), \\ \Pi_I(\alpha) &\longmapsto \Pi_I(\alpha^g), \end{aligned}$$

and $\rho_I(G) \leqslant \mathrm{Aut}(H(I, q))$. This proves a useful way of obtaining smaller completely transitive codes as we have the following theorem.

THEOREM 5.1. *Let C be a G-completely transitive code with covering radius t in the graph $H(m,q)$ and let I be a G-invariant subset of M. Then $\Pi_I(C)$ is a G-completely transitive code with covering radius r in the graph $H(I,q)$, where the action of G on $H(I,q)$ is given by ρ_I, and $(\Pi_I(C))_i = \Pi_I(C_i)$ for all $i \leq r$.*

PROOF. It is straightforward to check that $\Pi_I(C)$ is G-invariant (relative to ρ_I). Moreover, for all $\alpha, \beta \in \Pi_I(C)$ there exist $\alpha', \beta' \in C$ such that $\Pi_I(\alpha') = \alpha$ and $\Pi_I(\beta') = \beta$. Then as C is a G-orbit , there exists $g \in G$ such that $(\alpha')^g = \beta'$. Let $\overline{g} = \rho_I(g)$. Then $\alpha^{\overline{g}} = \beta$. Therefore $\Pi_I(C)$ is a $\rho_I(G)$-orbit.

Now $\Pi_I(C)$ has distance partition

$$\{\Pi_I(C), (\Pi_I(C))_1, \ldots, (\Pi_I(C))_r\}$$

for some $r \leq t$. We need to prove that $(\Pi_I(C))_i$ is a $\rho_I(G)$-orbit for all $1 \leq i \leq r$.

Since $\Pi_I(C)$ is a $\rho_I(G)$-orbit, $(\Pi_I(C))_i$ is fixed setwise by $\rho_I(G)$ for each $i = 1, \ldots, r$. By Lemma 5.1, for $\alpha \in (\Pi_I(C))_i$ there exists $\alpha' \in C_i$ such that $\Pi_I(\alpha') = \alpha$. Let $\beta \in \Pi_I(C_i)$. Then there exists $\beta' \in C_i$ such that $\Pi_I(\beta') = \beta$. Since C_i is a G-orbit, there exists $g \in G$ such that $(\alpha')^g = \beta'$. So if we let $\overline{g} = \rho_I(g)$, we have $\alpha^{\overline{g}} = \beta$. This implies that $\beta \in (\Pi_I(C))_i$ since $(\Pi_I(C))_i$ is invariant under $\overline{g}$, and hence $\Pi_I(C_i) = (\Pi_I(C))_i$. It also implies that $(\Pi_I(C))_i$ is a $\rho_I(G)$-orbit and hence $\Pi_I(C)$ is a G-completely transitive code. □

In many cases it turns out that the projection is a complete code, that is, $\Pi_I(C) = Q^I$.

PROPOSITION 5.1. *Let $G \leqslant S_q \mathrm{wr} S_m$ and C be a G-completely transitive code in $H(m,q)$ which is not of transitive type. Let the orbits of G on entries be $B_1, \ldots, B_s$ where $s \geq 2$. Then $\Pi_{B_i}(C) = Q^{B_i}$ for at least $s-1$ of the B_i-orbits.*

PROOF. Without loss of generality, we may suppose that $\Pi_{B_i}(C) = Q^{B_i}$ for the first k orbits of G for some $0 \leq k \leq s$ and $\Pi_{B_j}(C) \neq Q^{B_j}$ for $k+1 \leq j \leq s$. We need to prove that $k \geq s-1$. Suppose to the contrary that $k \leq s-2$.

Let $\alpha \in C$. We shall write α as $(\alpha_1, \ldots, \alpha_s)$ where $\alpha_i \in \Pi_{B_i}(C)$. Since $k < s$, there exists $\beta_s \in (\Pi_{B_s}(C))_1$. Now by Theorem 5.1, $\Pi_{B_s}(C)$ is a completely transitive code and hence is completely regular. Therefore we may choose β_s such that $\beta_s \sim \alpha_s$. So let $\beta = (\alpha_1, \ldots, \alpha_{s-1}, \beta_s)$. Then $\beta \sim \alpha$ but there does not exist $g \in G$ such that $\alpha^g = \beta$ as β_s is not in the orbit of $\rho_{B_s}(G)$ containing α_s. Therefore $\beta \in C_1$.

Similarly if $k < s-1$, there exists $\beta_{s-1} \in (\Pi_{B_{s-1}}(C))_1$ such that $\beta_{s-1} \sim \alpha_{s-1}$. So let $\gamma = (\alpha_1, \ldots, \alpha_{s-2}, \beta_{s-1}, \alpha_s)$. Then $\gamma \sim \alpha$ and there does not exist $g \in G$ such that $\alpha^g = \gamma$ as β_{s-1} is not in the orbit of $\rho_{B_{s-1}}(G)$ containing α_{s-1}. Therefore $\gamma \in C_1$ and so there exists $g \in G$ such that $\beta^g = \gamma$. However this contradicts β_s not being in the same orbit of $\rho_{B_s}(G)$ as α_s. Therefore $k \geq s-1$. □

We extend this result to obtain an explicit description of the structure of completely transitive codes with incomplete completely transitive projections.

THEOREM 5.2. *Let C be a G-completely transitive code in the graph $H(m,q)$ and let I be a G-invariant subset of M such that $\Pi_I(C) \neq Q^I$. Then $C = \Pi_I(C) \times Q^{M \setminus I}$.*

PROOF. Without loss of generality, we may assume that $I = \{1, \ldots, k\}$. Note that $C \subseteq \Pi_I(C) \times Q^{M \setminus I}$. By Theorem 5.1, $(\Pi_I(C))_1 = \Pi_I(C_1)$ and hence $C_1 \subseteq (\Pi_I(C))_1 \times Q^{M \setminus I}$.

Recall that Q_i denotes the ith direct factor in the decomposition $Q^m = Q_1 \times \cdots \times Q_m$, see Eqn. (1). Let $\alpha = (\alpha_1, \ldots, \alpha_m) \in C$, let $\gamma_{k+1} \in Q_{k+1} \backslash \{\alpha_{k+1}\}$, and set

$$\xi_{k+1} = (\alpha_1, \ldots, \alpha_k, \gamma_{k+1}, \alpha_{k+2}, \ldots, \alpha_m).$$

Then $d(\alpha, \xi_{k+1}) = 1$ and $\xi_{k+1} \in \Pi_I(C) \times Q^{M \backslash I}$. So $\xi_{k+1} \notin C_1$ and therefore $\xi_{k+1} \in C$.

Similarly, if $k + 2 \leq m$, then for $\gamma_{k+2} \in Q_{k+2} \backslash \{\alpha_{k+2}\}$, the m-tuple

$$\xi_{k+2} = (\alpha_1, \ldots, \alpha_k, \gamma_{k+1}, \gamma_{k+2}, \alpha_{k+3}, \ldots, \alpha_m)$$

lies in C. Proceeding inductively we see that

$$(\alpha_1, \ldots, \alpha_k) \times Q^{M \backslash I} \subseteq C,$$

where $(\alpha_1, \ldots, \alpha_k) \times Q^{M \backslash I} = \{(\alpha_1, \ldots, \alpha_k, \gamma) : \gamma \in Q^{M \backslash I}\}$, and this holds for all $(\alpha_1, \ldots, \alpha_k) \in \Pi_I(C)$. Therefore $\Pi_I(C) \times Q^{M \backslash I} \subseteq C$ and so $C = \Pi_I(C) \times Q^{M \backslash I}$. □

The decomposition given in Theorem 5.2 suggests a possible reconstruction method which produces infinitely many such codes.

THEOREM 5.3. *Let C be a G-completely transitive code in the graph $H(m, q)$ and let $J = \{m + 1, \ldots, m + k\}$. Let $\overline{G} = G \times (S_q \mathrm{wr} S_k)$ and $\overline{C} = C \times Q^J$. Then $\overline{C}$ is a $\overline{G}$-completely transitive code in the graph $H(m + k, q)$.*

PROOF. Let $i \leq t$, and let $\beta = (\beta', \beta_{m+1}, \ldots, \beta_{m+k}) \in C_i \times Q^J$. By definition of C_i, there exists $\alpha' = (\alpha_1, \ldots, \alpha_m) \in C$ such that $d(\alpha', \beta') = i$. Then

$$\gamma = (\alpha', \beta_{m+1}, \ldots, \beta_{m+k}) \in \overline{C},$$

and $d(\gamma, \beta) = d(\alpha', \beta') = i$, and so $d(\beta, \overline{C}) \leq i$.

Suppose there exists $\xi = (\xi_1, \ldots, \xi_{m+k}) \in \overline{C}$ such that $d(\beta, \xi) = j < i$. Then as $\overline{C} = C \times Q^J$, it follows that

$$\eta = (\xi_1, \ldots, \xi_m, \beta_{m+1}, \ldots, \beta_{m+k}) \in \overline{C},$$

and $d(\beta, \eta) = d(\beta', (\xi_1, \ldots, \xi_m)) \leq d(\beta, \xi) = j < i$, and hence $d(\beta', C) \leq j < i$ contradicting $\beta' \in C_i$. Therefore $d(\beta, \overline{C}) = i$ and hence $C_i \times Q^J \subseteq \overline{C}_i$ for all i.

On the other hand, if $\gamma \in \overline{C}_i \backslash (C_i \times Q^J)$, then $\gamma = (\gamma', \gamma_{m+1}, \ldots, \gamma_{m+k})$ with $\gamma' \notin C_i$. Since $d(\gamma, \overline{C}) = i$ and $\gamma' \notin C_i$ it follows that $j := d(\gamma', C) < i$ and hence $\gamma \in C_j \times Q^J \subseteq \overline{C}_j$, which is a contradiction. Hence $\overline{C}_i = C_i \times Q^J$. Since G is transitive on C_i and $S_q \mathrm{wr} S_k$ is transitive on Q^J it follows that $\overline{G}$ is transitive on $\overline{C}_i$. Hence $C \times Q^J$ is $\overline{G}$-completely transitive. □

We now have the following structure theorem for completely transitive codes in the Hamming Graphs. This was the main result of the first author's honours dissertation [4, Theorem 5.3.5] and Theorem 1.3 follows from it.

THEOREM 5.4. *Let C be a code in the graph $H(m, q)$. If C is G-completely transitive, then there exists a G-invariant subset I of M with complement K such that $C = C_I \times Q^K$, and one of*

(1) $I = \varnothing$; *or*
(2) C_I *is a* $\rho_I(G)$*-transitive,* $\rho_I(G)$*-completely transitive code in the graph* $H(I, q)$; *or*
(3) C_I *is a* $\rho_I(G)$*-nearly complete,* $\rho_I(G)$*-completely transitive code in* $H(I, q)$.

Conversely any code $C = C_I \times Q^K$ *with one of 1–3 true is* G*-completely transitive for* $G = \rho_I(G) \times (S_q \mathrm{wr} S_{|K|})$.

PROOF. The converse statement follows immediately from Theorem 5.3, so we only need to prove the forward implication. If C is the complete code, then we have case 1, so we may assume that C is not the complete code. Let s be the number of orbits of G on entries. If $s = 1$, then case 2 holds with $K = \varnothing$. We complete the proof by induction on s.

Assume that the result is true for $s = i$, for some $i \geq 1$, and let C be a G-completely transitive code in $H(m, q)$ with $s = i + 1$. Then, by Theorem 5.1 and Proposition 5.1, we may suppose that $\Pi_{B_j}(C) = Q^{B_j}$ for $j \leq i$. Let $J = B_1 \cup \ldots \cup B_i$. Then, by Theorem 5.1, $\Pi_J(C)$ is a G-completely transitive code in $H(n, q)$ where $n = m - |B_{i+1}|$. Suppose first that $\Pi_J(C) \neq Q^J$. Then, by the inductive hypothesis, $\Pi_J(C)$ satisfies case 3 since $\Pi_{B_j}(C) = Q^{B_j}$ for all $j \leq i$. So there exists a G-invariant subset, I of J, such that $\Pi_J(C) = C_I \times Q^L$ where $L = J \backslash I$ and C_I is a G-nearly-complete, G-completely transitive code in $H(I, q)$. Then, by Theorem 5.2, $C = C_I \times Q^L \times Q^{B_{i+1}}$ as in case 3.

Thus we may suppose that $\Pi_J(C) = Q^J$. If $\Pi_{B_{i+1}}(C) \neq Q^{B_{i+1}}$, then, by Theorem 5.2, $C = Q^J \times \Pi_{B_{i+1}}(C)$ as in case 2. So we may assume that $\Pi_{B_{i+1}}(C) = Q^{B_{i+1}}$. Let I be any union of i of the B_j. If $\Pi_I(C) \neq Q^I$, then arguing as above, we find that C is as in case 3. If there does not exist such an I, then C is a G-nearly-complete code, so case 3 holds with $K = \varnothing$. Therefore, by the principle of mathematical induction, the statement is true for all s. □

Thus to study completely transitive codes in $H(m, q)$, we just need to study nearly complete and transitive codes, and if all completely transitive codes of these types can be determined, then we have determined all completely transitive codes in the Hamming Graphs.

6. G-NEARLY COMPLETE CODES AND THEIR SECTIONS

In this section, we investigate G-nearly-complete, G-completely transitive codes and we show that these codes involve completely transitive codes of transitive type as sections. Our first result, Theorem 6.1, explores the structure of the distance partition of such a code. It requires the following lemma.

LEMMA 6.1. *Let* $G \leqslant S_q \mathrm{wr} S_m$ *and let* $I \subseteq M$ *be fixed setwise by the action of* G *on entries. If* $\varnothing \neq D \subseteq Q^m$ *is a* G*-orbit, then* $\Pi_I(D)$ *is a* $\rho_I(G)$*-orbit.*

PROOF. Let $\alpha \in \Pi_I(D)$ and let $\overline{g} \in \rho_I(G)$. Then there exist $\alpha' \in D$ and $g \in G$ such that $\Pi_I(\alpha') = \alpha$ and $\rho_I(g) = \overline{g}$. Then $(\alpha')^g \in D$ as D is a G-orbit, and hence $\alpha^{\overline{g}} = \Pi_I((\alpha')^g) \in \Pi_I(D)$. Hence $\Pi_I(D)$ is fixed setwise by $\rho_I(G)$.

Let $\alpha, \beta \in \Pi_I(D)$. Then there exist $\alpha', \beta' \in D$ such that $\Pi_I(\alpha') = \alpha$ and $\Pi_I(\beta') = \beta$. Since D is a G-orbit there exists $g \in G$ such that $(\alpha')^g = \beta'$. Let $\overline{g} = \rho_I(g)$. Then $\overline{g} \in \rho_I(G)$ and $\alpha^{\overline{g}} = \Pi_I((\alpha')^g) = \beta$, so $\Pi_I(D)$ is a $\rho_I(G)$-orbit. □

THEOREM 6.1. *Let C be a G-nearly-complete, G-completely transitive code in the graph $H(m, q)$ with covering radius t. Then for all $i = 0, \ldots, t$, we have that C_i is a G-nearly-complete code.*

PROOF. Let $i \leq t$ and let I be a proper G-invariant subset of M. Since C is G-nearly-complete, $\Pi_I(C) = Q^I$. So, by Theorem 5.1, $\rho_I(G)$ is transitive on Q^I. By Lemma 6.1, $\Pi_I(C_i)$ is a $\rho_I(G)$-orbit and so, since $\rho_I(G)$ is transitive on Q^I, we have $\Pi_I(C_i) = Q^I$. As this holds for all such I, C_i is a G-nearly-complete code. □

Let C be a G-completely transitive code with covering radius t. Let J be a proper subset of M, and let $\beta = (\beta_1, \ldots, \beta_m) = (\beta_J, \beta_{M\setminus J}) \in C$. Then we write

$$Q^J \times \beta_{M\setminus J} = \{(\delta, \beta_{M\setminus J}) : \delta \in Q^J\},$$

and, more generally, for $D \subseteq Q^J$ we write

$$D \times \beta_{M\setminus J} = \{(\delta, \beta_{M\setminus J}) : \delta \in D\}.$$

For each $i = 0, \ldots, t$, set

$$C_i(\beta, J) = \{\delta \in Q^J : (\delta, \beta_{M\setminus J}) \in C_i\}.$$

Note that $C_i(\beta, J) \times \beta_{M\setminus J} = C_i \cap (Q^J \times \beta_{M\setminus J})$. We then have the following definition.

DEFINITION. We call $C_0(\beta, J)$ the *section of C with respect to β and J* and we will often denote this as $C(\beta, J)$.

We define $G(\beta, J)$ to be the setwise stabilizer in G of $Q^J \times \beta_{M\setminus J}$. Then since C_i is G-invariant, $G(\beta, J)$ is also the setwise stabilizer in G of $C_i(\beta, J) \times \beta_{M\setminus J}$ for each $i = 0, \ldots, t$. If we suppose that J is G-invariant, then for each $g \in G(\beta, J)$ we can define a map $\varphi_J(g) : Q^J \longrightarrow Q^J$ as follows: for $\delta \in Q^J$, $\delta^{\varphi_J(g)}$ is the element of Q^J such that

$$(\delta, \beta_{M\setminus J})^g = (\delta^{\varphi_J(g)}, \beta_{M\setminus J}).$$

Then the homomorphism

$$\begin{array}{rcl} \varphi_J : G(\beta, J) & \longrightarrow & \mathrm{Aut}(H(J, q)) \\ g & \longmapsto & \varphi_J(g) \end{array}$$

is a permutation representation. Relative to this action, we show that $C(\beta, J)$ is a $G(\beta, J)$-completely transitive code in $H(J, q)$.

THEOREM 6.2. *Let C be a G-nearly-complete, G-completely transitive code in the graph $H(m, q)$ with covering radius $t \geq 1$. Let $\beta \in C$ and let J be a proper G-invariant subset of M. Then $C(\beta, J)$ is a $G(\beta, J)$-completely transitive code with the same covering radius t and for each $i = 0, \ldots, t$, $(C(\beta, J))_i = C_i(\beta, J)$.*

PROOF. By Theorem 6.1, for each $i = 0, \ldots, t$, we have $\Pi_{M\setminus J}(C_i) = Q^{M\setminus J}$ and hence $C_i(\beta, J) \neq \varnothing$. Also the sets $C_i(\beta, J)$ partition Q^J, and as discussed above, each $C_i(\beta, J)$ is left invariant by $\varphi_J(G(\beta, J))$.

Let $\delta, \eta \in C_i(\beta, J)$. Then $(\delta, \beta_{M\setminus J}), (\eta, \beta_{M\setminus J}) \in C_i$. Therefore there exists $g \in G$ such that $(\delta, \beta_{M\setminus J})^g = (\eta, \beta_{M\setminus J})$. Then $g \in G(\beta, J)$ as J is G-invariant, therefore $\delta^{\varphi_J(g)} = \eta$ and so each $C_i(\beta, J)$ is a $\varphi_J(G(\beta, J))$-orbit.

Let $i = 0, \ldots, t$, and let $\delta \in C_i(\beta, J)$. Then $(\delta, \beta_{M\setminus J}) \in C_i$, and for all $\gamma \in C(\beta, J)$ we have

$$d(\gamma, \delta) = d((\gamma, \beta_{M\setminus J}), (\delta, \beta_{M\setminus J})) \geq d(C, (\delta, \beta_{M\setminus J})) = i.$$

Therefore $\delta \in (C(\beta, J))_{i'}$ for some $i' \geq i$. In particular, the covering radius t' of $C(\beta, J)$ satisfies $t' \geq t$. Now as $C_i(\beta, J)$ is a $\varphi_J(G(\beta, J))$-orbit and $\varphi_J(G(\beta, J))$ leaves each $(C(\beta, J))_k$ invariant we have that

$$C_i(\beta, J) \subseteq (C(\beta, J))_{i'}. \tag{2}$$

We now use induction on i to show that $C_i(\beta, J) = (C(\beta, J))_i$. By definition $C(\beta, J) = C_0(\beta, J)$, so $0' = 0$. Now suppose that for some $k = 0, \ldots, t-1$, $C_i(\beta, J) = (C(\beta, J))_i$ for all $i \leq k$. Then

$$\bigcup_{0\leq i\leq k} (C(\beta, J))_i = \bigcup_{0\leq i\leq k} C_i(\beta, J) \neq Q^J$$

since $k < t \leq t'$ and consequently $(C(\beta, J))_{k+1} \neq \varnothing$. Now for all $\delta \in (C(\beta, J))_{k+1}$, there exists $\gamma \in C(\beta, J)$ such that $d((\delta, \beta_{M\setminus J}), (\gamma, \beta_{M\setminus J})) = k+1$ and so, $\delta \in C_j(\beta, J)$ for some $j \leq k+1$. However since $C_i(\beta, J) = (C(\beta, J))_i$ for all $i \leq k$, it follows that $(C(\beta, J))_{k+1} \subseteq C_{k+1}(\beta, J)$ and so by equation (2), we have that $(C(\beta, J))_{k+1} = C_{k+1}(\beta, J)$. Then, by the principle of induction, we have that $C_i(\beta, J) = (C(\beta, J))_i$ for all $i = 0, \ldots, t$. □

We should also note the following lemma concerning G-nearly-complete codes:

LEMMA 6.2. *Let C be a G-nearly-complete code in $H(m, q)$ with covering radius t and let k be the size of the smallest orbit of G acting on entries. Then $t \leq k$.*

PROOF. Without loss of generality, we may assume that the smallest orbit of G acting on entries is $I_1 = \{1, \ldots, k\}$. Let $\gamma = (\gamma_1, \ldots, \gamma_m)$ be any vertex in C_t. Then as C is G-nearly-complete there exists $\beta = (\beta_1, \ldots, \beta_k, \gamma_{k+1}, \ldots, \gamma_m) \in C$. Therefore $d(\gamma, \beta) \leq k$ and so $t \leq k$. □

We are now in a position to prove that every G-nearly-complete, G-completely transitive code has a section $C(\beta, J)$ which is a $G(\beta, J)$-transitive, $G(\beta, J)$-completely transitive code.

THEOREM 6.3. *Let C be a G-nearly-complete, G-completely transitive code with covering radius $t \geq 1$ in the graph $H(m, q)$ and let $\beta \in C$. Then, there exists a proper subset J of M and a section $C(\beta, J)$ of C such that $C(\beta, J)$ is a $G(\beta, J)$-transitive, $G(\beta, J)$-completely transitive code with covering radius t.*

PROOF. Without loss of generality, we may assume that the orbits of G on entries are

$$I_1 = \{1, \ldots, k\}, I_2 = \{k+1, \ldots, l\}, \ldots, I_s = \{j+1, \ldots, m\}$$

where $|I_1| \leq |I_2| \leq \cdots \leq |I_s|$, and $s \geq 2$. Let $\beta \in C$. Then, by Theorem 6.2, $C(\beta, I_1)$ is a $G(\beta, I_1)$-completely transitive code of covering radius t and for all $i = 0, \ldots, t$, $(C(\beta, I_1))_i = C_i(\beta, I_1)$. By Theorem 5.4,

$$C(\beta, I_1) = C_L \times Q^K,$$

where L is a $G(\beta, I_1)$-invariant subset of I_1 with complement K and either

- $L = \varnothing$, or
- $K = \varnothing$ and C_L is a $G(\beta, I_1)$-transitive, $G(\beta, I_1)$-completely transitive code in $H(L, q)$ of covering radius t, or
- $K = \varnothing$ and C_L is a $G(\beta, I_1)$-nearly complete, $G(\beta, I_1)$-completely transitive code in $H(L, q)$ of covering radius t, or
- $K \neq \varnothing$ and C_L is a $G(\beta, I_1)$-transitive, $G(\beta, I_1)$-completely transitive code in $H(L, q)$ of covering radius t, or
- $K \neq \varnothing$ and C_L is a $G(\beta, I_1)$-nearly complete, $G(\beta, I_1)$-completely transitive code in $H(L, q)$ of covering radius t.

If $L = \varnothing$, then $C(\beta, I_1) = Q^{I_1}$ and has covering radius 0, which is a contradiction. Therefore $L \neq \varnothing$.

Note that

$$\begin{aligned} C(\beta, L) &= \{\delta \in Q^L : (\delta, \beta_{M\setminus L}) \in C\} \\ &= \{\delta \in Q^L : (\delta, \beta_{I_1\setminus L}) \in C(\beta, I_1)\} \\ &= C_L. \end{aligned}$$

Also for $g \in G(\beta, L)$ we have

$$(\delta, \beta_{I_1\setminus L}, \beta_{M\setminus I_1})^g = (\eta, \beta_{I_1\setminus L}, \beta_{M\setminus I_1}),$$

for some $\eta \in Q^L$. Then since I_1 is G-invariant g must stabilize $Q^{I_1} \times \beta_{M\setminus I_1}$ and so $g \in G(\beta, I_1)$. Hence $G(\beta, L)$ is the stabilizer of $Q^L \times \beta_{I_1\setminus L}$ in $G(\beta, I_1)$.

Now suppose that $K = \varnothing$. Then if C_L is a $G(\beta, I_1)$-transitive, $G(\beta, I_1)$-completely transitive code in $H(L, q)$, L is our desired subset. So we may assume that C_L is a $G(\beta, I_1)$-nearly complete, $G(\beta, I_1)$-completely transitive code in $H(L, q)$. Let N be the smallest orbit of $G(\beta, I_1)$ on the entries of L. Then $C(\beta, N) \times \beta_{I_1\setminus N} = C(\beta, I_1) \cap (Q^N \times \beta_{I_1\setminus N})$ and $G(\beta, N)$ is equal to the stabilizer in $G(\beta, I_1)$ of $Q^N \times \beta_{M\setminus N}$. Then, by Theorem 6.2 applied to the $G(\beta, I_1)$-nearly complete, $G(\beta, I_1)$-completely transitive code $C(\beta, I_1)$ with covering radius t, $C(\beta, N)$ is a $G(\beta, N)$-completely transitive code in $H(N, q)$ with covering radius t and we can again apply Theorem 5.4. We temporarily interrupt consideration of this case and consider together the two possibilities where $K \neq \varnothing$.

Suppose $K \neq \varnothing$. Now for all $i = 0, \ldots, t$, we have that $C_i = (C_L)_i \times Q^K$ and hence $C_i(\beta, L) = (C_L)_i = (C(\beta, L))_i$. Also, as discussed earlier, $G(\beta, L)$ is equal to the stabilizer of $Q^L \times \beta_{I_1\setminus L}$ in $G(\beta, I_1)$. Then the sets $C_i(\beta, L)$ partition Q^L and are invariant under $G(\beta, L)$ as each C_i is invariant under G. Let $\delta, \eta \in C_i(\beta, L)$, then $(\delta, \beta_{I_1\setminus L})$ and $(\eta, \beta_{I_1\setminus L}) \in C_i(\beta, I_1)$. Therefore, there exists $g \in G(\beta, I_1)$ such that $(\delta, \beta_{I_1\setminus L})^g = (\eta, \beta_{I_1\setminus L})$. Then as L is $G(\beta, I_1)$-invariant, $g \in G(\beta, L)$. Therefore each $C_i(\beta, L)$ is a $G(\beta, L)$-orbit and so $C(\beta, L)$ is a $G(\beta, L)$-completely transitive code in $H(L, q)$ with covering radius t. Then, Theorem 5.4 applies again. Thus, whether or not K is empty, either we find an appropriate section or we are in a situation where we can apply Theorem 5.4 to a $G(\beta, L)$-completely transitive section $C(\beta, L)$ of the same covering radius t, and with shorter length $|L| < m$.

If we continue this process, since m is finite we will eventually find a subset $J \subseteq I_1$ such that $C(\beta, J)$ is a $G(\beta, J)$-transitive, $G(\beta, J)$-completely transitive code and with covering radius t. □

We then use Theorem 6.3 to prove the following from which Theorem 1.4 immediately follows:

THEOREM 6.4. *For every G-completely transitive code C with covering radius $t \geq 1$ in the graph $H(m, q)$, and for each $\beta \in C$, there exists a subset J of M such that the section $C(\beta, J)$ is a $G(\beta, J)$-transitive, $G(\beta, J)$-completely transitive code with covering radius t.*

PROOF. Since G is transitive on C, we need only prove the result for a fixed codeword $\beta \in C$. By Theorem 5.4, and since $t \geq 1$, we know that:

$$C = C_L \times Q^K$$

where L is G-invariant and either

- C_L is a G-transitive, G-completely transitive code in $H(L, q)$ with covering radius t, or
- C_L is a G-nearly-complete, G-completely transitive code in $H(L, q)$ with covering radius t.

Arguing as in the penultimate paragraph of the proof of Theorem 6.3, $C_L = C(\beta, L)$ is $G(\beta, L)$-completely transitive. If $C(\beta, L)$ is $G(\beta, L)$-transitive, $C(\beta, L)$ is the required section. Otherwise, we proceed as in the proof of Theorem 6.3 □

We now know that every completely transitive code in a Hamming graph involves a completely transitive code of transitive type in a possibly smaller Hamming graph, but having the same covering radius. This suggests that the completely transitive codes we should investigate are those of transitive type and if we learn enough about them, we may be able to determine the possibilities for nearly complete codes also.

ACKNOWLEDGEMENT

M. Giudici was supported by the Australian Research Council Grant A69800706 during the preparation of this paper.

REFERENCES

1. N. L. Biggs and A. T. White, *Permutation groups and combinatorial structures*, London Mathematical Society Lecture Note Series **33**, Cambridge University Press, Cambridge, 1979.
2. A. E. Brower, A. M. Cohen and A. Neumaier, *Distance Regular Graphs*, Springer-Verlag, 1989.
3. J. Cannon and C. Playoust, *An Introduction to MAGMA*, School of Mathematics and Statistics, University of Sydney, Australia, NSW 2006, 1995.
4. M. Giudici, Completely transitive codes, Honours dissertation, Department of Mathematics, The University of Western Australia, 1997.
5. M. Giudici, Completely transitive codes in Hamming graphs, Masters thesis, Department of Mathematics, The University of Western Australia, 1998.
6. C. D. Godsil, *Algebraic combinatorics*, Chapman and Hall Mathematics, Chapman and Hall, New York, 1993.
7. C. D. Godsil and C. E. Praeger, Completely transitive designs, 1997, Preprint
8. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-correcting Codes*, North-Holland Mathematical Library, North-Holland, Amsterdam, 1977.
9. A. Neumaier, Completely regular codes, *Discrete Math.*, **106/107** (1992), 353–360.
10. P. Solé, Completely regular codes and completely transitive codes, *Discrete Math.*, **81** (1990), 193–201.

MICHAEL GIUDICI AND CHERYL E. PRAEGER
Department of Mathematics,
The University of Western Australia,
Nedlands WA 6907,
Australia
E-mail: M.Giudici@qmw.ac.uk,
praeger@maths.uwa.edu.au